

DRAFT DOCUMENT – PREDECISIONAL

INFORMATION COLLECTION SUPPORTING STATEMENT

Minimum Standards for Driver’s licenses and Identification Cards Acceptable by Federal Agencies for Official Purposes

OMB Control No. _____

- 1. Explain the circumstances that make the collection of information necessary. Identify any legal or administrative requirements that necessitate the collection. Attach a copy of the appropriate section of each statute and regulation mandating or authorizing the collection of information. (Annotate the CFR parts/sections affected).**

REAL ID Act and Notice of Proposed Rulemaking

The REAL ID Act of 2005 (the Act) prohibits Federal agencies from accepting State-issued drivers’ licenses or identification cards (DL/ID) for official purposes – defined by the Act as boarding commercial aircraft, accessing Federal facilities, entering nuclear power plants, and any other purposes as determined by the Secretary – unless the DL/ID is issued by a State that meets the requirements set forth in the Act.¹ The regulations, which DHS issued in January 2008, establish the minimum standards that States must meet to comply with the Act.² These include requirements for presentation and verification of documents to establish identity and lawful status, standards for document issuance and security, and physical security requirements for driver’s license production facilities. In addition, under the regulations, beginning May 7, 2025, Federal agencies will be prohibited from accepting a State-issued card for official purposes unless the card is compliant with the REAL ID Act and regulations.³ This is known as “card-based enforcement.”

As both the REAL ID Act and regulations were issued before the inception of mDLs, they do not address digital versions of State-issued driver’s licenses or State-issued identification cards, which are known collectively as “mobile driver’s licenses” (mDLs). In December 2020, the REAL ID Modernization Act clarified that mDLs are subject to REAL ID requirements by amending the definitions of “driver’s license” and “identification card” to specifically include mDLs that have been issued in accordance with regulations prescribed by the Secretary.⁴ Although the current regulations set forth card security requirements, such as physical security features to deter fraud and tampering,⁵ many of these requirements do not apply to mDLs, which prevents States from issuing REAL ID-compliant mDLs.

¹ The REAL ID Act of 2005—Title II of division B of the FY05 Emergency Supplemental Appropriations Act, as amended, Public Law 109– 13, 49 U.S.C. 30301 note.

² See 73 FR 5272 (Jan. 29, 2008) and 6 CFR part 37.

³ See 6 CFR 37.5(b).

⁴ Sec. 1001 of the REAL ID Modernization Act, Title X of Division U of the Consolidated Appropriations Act, 2021, Pub. L. No. 116-260, 134 Stat. 2304, available at [Public Law 116 - 260 - Consolidated Appropriations Act, 2021 - Content Details - \(govinfo.gov\)](https://www.govinfo.gov/records/public-law-116-260-consolidated-appropriations-act-2021-content-details).

⁵ 6 CFR §§ 37.15(c) & 37.17(h).

Accordingly, DHS is conducting a rulemaking to amend the regulations to address mDLs. DHS is conducting this rulemaking incrementally, in two phases. In its first phase, DHS is publishing a Notice of Proposed Rulemaking (NPRM) to amend the REAL ID regulations to waive, on a temporary and State-by-State basis, the card-based requirement in Sec. 37.5(b). The temporary waiver enabled by this rule would permit Federal agencies, at their discretion, to continue accepting, for official purposes as defined in the Act and regulations, mDLs (1) from individuals who have been issued a valid and unexpired REAL ID-compliant physical driver's license or identification card, and (2) issued by States that DHS has determined to be REAL ID-compliant to whom DHS has issued a waiver. In the second phase rulemaking, DHS intends to issue comprehensive requirements for mDLs after emerging industry standards and Federal guidelines are finalized, and at that time would repeal the waiver provisions established in this rule. This dual-phased rulemaking is necessary because DHS believes it is premature to issue comprehensive requirements while multiple standards and guidelines are pending.

New section 37.7 of the proposed rule would establish a limited and temporary process for DHS to issue to States a waiver that exempts their mDLs from meeting the card-based compliance requirement of section 37.5(b). This waiver would authorize Federal agencies to accept a State's mDL for official purposes, but only if in addition to the waiver, the mDL holder has been issued a valid and unexpired REAL ID-compliant physical card by a State that is otherwise in full compliance with applicable REAL ID requirements. The certificate of waiver would include the dates of effectiveness and expiration, and any other terms and conditions as necessary, and would be valid for three years. The waiver would also require a State that receives a waiver to continue complying with all requirements of the REAL ID Act, 6 CFR 37.51(a), and any terms and conditions specified in the certificate of waiver.

The proposed changes would apply to State driver's licensing agencies issuing mDLs who seek a temporary waiver from DHS for their mDLs. The waiver would enable Federal agencies to accept such mDLs for official purposes, defined in the REAL ID Act as accessing Federal facilities, entering nuclear power plants, boarding Federally regulated commercial aircraft, and any other purposes that the Secretary shall determine. Any Federal agency that chooses to accept mDLs for official purposes must procure a reader in order to receive an individual's identity data. The proposed rule would not impose any requirements on: States that do not seek a waiver for mDLs; non-State issuers of other forms of digital identification; or Federal agencies that choose not to accept mDLs.

Mobile Driver's Licenses Generally

An mDL is generally recognized as the digital representation of an individual's identity information contained on a State-issued physical DL/ID.⁶ An mDL may be stored on a diverse range of portable or mobile electronic devices, such as smartphones, smartwatches, and storage devices containing memory. Like a physical card, mDL data originates from identity information about an individual that is maintained in the database of a State driver's licensing agency.

⁶ A technical description of mDLs as envisioned by the American Association of Motor Vehicle Administrators may be found at <https://www.aamva.org/Mobile-Drivers-License/>.

Mobile driver's license issuance is proliferating rapidly among States, with nearly half of all States piloting, issuing, or considering mDLs. As of the date of this document, at least eight States (Arizona, Colorado, Delaware, Louisiana, Maryland, Mississippi, Oklahoma, and Utah) are issuing mDLs, and three States (Florida, Iowa, Utah) are currently piloting or have piloted mDLs. Additionally, at least 17 States (California, District of Columbia, Georgia, Hawaii, Illinois, Indiana, Kentucky, Michigan, Missouri, New Jersey, New York, North Dakota, Pennsylvania, Puerto Rico, Tennessee, Texas, and Wyoming) have indicated they are studying mDLs or considering enabling legislation.

Collections of Information Under this NPRM: States

The NPRM proposes various collections of information from States that are subject to the Paperwork Reduction Act (PRA). States will be required to submit information to DHS as part of their applications for a certificate of waiver for mDLs, in compliance with reporting requirements, and in response to DHS notices of suspension and termination.

(a) Submission of Initial Application and Audit Report

A State seeking a certificate of waiver must follow the application process set forth in new section 37.9(a) of the proposed rule. Specifically, a State must file a complete application as set forth in sections 37.10(a) and (b) of the proposed rule. Section 37.10(a) (and accompanying Appendix A) sets forth all information, documents, and data that a State must include in its application, and section 37.10(b) requires a State to submit a report prepared by an independent auditor verifying the accuracy of the information provided by the State in response to section 37.10(a). To assist States that are considering applying for a waiver, DHS has developed guidelines, entitled, "Mobile Driver's License Waiver Application Guidance," which provide non-binding recommendations of some ways that States can meet the application requirements set forth in the rule.

New section 37.9(b) establishes a timeline for DHS to issue decisions on a waiver application. Under this section, DHS would endeavor to provide a decision on initial applications within 60 days, but not longer than 90 days. DHS would provide three types of notice: approved, insufficient, or denied. States that are granted a waiver would be included in a list of State-mDLs approved for Federal use, published by DHS at www.dhs.gov/real-id/mDL.

(b) Supplemental Submissions

DHS may notify a State that its application is insufficient upon finding that an application did not respond to certain information or contains other deficiencies. In this instance, DHS would provide States an explanation of such deficiencies and afford them an opportunity to address deficiencies and submit supplemental information. DHS would permit States to submit multiple amended applications if necessary, with the intent of working with States individually to enable their mDLs to comply with waiver criteria. States would have 60 days to submit supplemental information.

(c) Request for Reconsideration of Denied Application

If DHS denies an application, DHS would provide States the specific grounds for the basis of the denial and afford them an opportunity to seek reconsideration of a denied application. A State would have 90 days to file a request for reconsideration, explaining what corrective actions it intends to implement, or explain why the denial is incorrect.

(d) Re-Application

A State whose request for reconsideration has been denied may choose to submit a new application. In addition, a State that seeks to renew a certificate of waiver that has expired must submit a new application. As discussed in paragraph (g), below, a State to whom DHS has issued a final suspension or termination may apply for a new waiver.

(e) Reporting of Significant Modifications to mDL Issuance Processes

Under new section 37.9(e)(2), a State must report to DHS if the State, after receiving a certificate of waiver, makes significant modifications to its mDL issuance processes that differ in a material way from information that the State provided in its application. States must provide written notice of such changes to DHS at www.dhs.gov/real-id/mDL 60 days before implementing such changes. This requirement is intended to apply to changes that may undermine the bases under which DHS granted a waiver. The reporting requirement is not intended to apply to routine, low-level changes, such as software updates and patches.

(f) Reporting of Discovery of Significant Cyber Incident or Breach

Under section 8.6 of Appendix A, States are required to provide written notice to DHS at www.dhs.gov/real-id/mDL within 72 hours of the discovery of a significant cyber incident or breach which may compromise the integrity of State Certificate Systems.

(g) Responses to DHS Notices of Suspension and Termination

New section 37.9(e)(4) of the proposed rule sets forth processes for suspension of certificates of waiver. DHS may suspend a certificate of waiver if DHS determines that a State: (1) failed to comply with any terms and conditions specified in the certificate of waiver, (2) failed to comply with reporting requirements, or (3) issues mDLs in a manner that is not consistent with the information the State provided in its application. Before suspending a waiver for these reasons, DHS will provide such State written notice via email that it intends to suspend its waiver, along with an explanation of the reasons, information on how the State may address the deficiencies. States will have 30 days to respond, and DHS will respond to the State via email within 30 days. DHS may withdraw the suspension notice, issue a final suspension, or request additional information from the State.

In addition, DHS may suspend a waiver at any time upon discovery of imminent or serious threats to security, privacy, or data integrity, such as cyber-attacks and other events that

cause serious harm to Federal agencies, such as cyber-attacks on a State's mDL issuance processes that compromise the integrity of its mDLs. If DHS determines such suspension is necessary, DHS will provide written notice via email to each State whose certificate of waiver is affected, as soon as practicable after discovery of the triggering event, providing an explanation for the suspension, as well as an estimated timeframe for resumption of the validity of the certificate of waiver. A State that has been issued a final suspension may seek to apply for a new certificate of waiver by submitting a new application.

New section 37.9(e)(5) proposes that DHS may terminate a certificate of waiver for specified violations, including: (1) failure to comply with REAL ID requirements in section 37.51(a) of this part, (2) egregious violations of any terms and conditions specified in the certificate of waiver that the State is unwilling to cure, (3) egregious violation of reporting requirements that the State is unwilling to cure, and (4) providing false information in its waiver application. Before terminating a certificate of waiver, DHS would provide via email written notice of intent to terminate, including findings supporting the termination and an opportunity to present information. A State would have seven days to respond to the notice, and DHS would respond via email within 30 days. A State whose certificate of waiver has been terminated may apply for a new certificate of waiver by submitting a new application.

2. *Indicate how, by whom, and for what purpose the information is to be used. Except for a new collection, indicate the actual use the agency has made of the information received from the current collection.*

As discussed above, the proposed rule would establish a limited and temporary process for States to apply to DHS for a certificate of waiver that would exempt their mDLs from meeting the card-based compliance requirement of section 37.5(b). The collection of the information will enable DHS to issue a waiver to States, which would authorize Federal agencies to accept, at their discretion, a State's mDL for official purposes. DHS will use all of the submitted documentation to evaluate a State's request for a waiver. The proposed rule would require the following information collections from States:

- (a) Submission of an initial waiver application, including audit report;
- (b) Supplemental submissions for applications deemed insufficient;
- (c) Requests for reconsideration of applications subject to a notice of denial;
- (d) Submission of a new application for: initial applications that have been denied, to renew an expired waiver, or waivers that have been suspended or terminated;
- (e) Reporting requirements for significant modifications that a State makes to its mDL issuance processes that materially differ from information that the State provided in its application that was the basis of an issued waiver;
- (f) Reporting requirements for discovery of a significant cyber incident or breach which may compromise the integrity of State Certificate Systems; and
- (g) Responses to DHS notices of suspension or termination.

All of the items above are considered new information collections.

3. ***Describe whether, and to what extent, the collection of information involves the use of automated, electronic, mechanical, or other technological collection techniques or other forms of information technology, e.g., permitting electronic submission of responses, and the basis for the decision for adopting this means of collection. Also describe any consideration of using information technology to reduce burden. [Effective 03/22/01, your response must SPECIFICALLY reference the Government Paperwork Elimination Act (GPEA), which addresses electronic filing and recordkeeping, and what you are doing to adhere to it. You must explain how you will provide a fully electronic reporting option by October 2003, or an explanation of why this is not practicable.]***

In compliance with GPEA, States will be permitted to electronically submit the information for their waiver applications. The final rule does not define specific format submission requirements for States. States will be permitted to submit electronic signatures but must keep the original signature on file.

4. ***Describe efforts to identify duplication. Show specifically why any similar information already available cannot be used or modified for use for the purpose(s) described in Item 2 above.***

This information will be collected directly from the States to assist DHS in making determinations on applications for a temporary certificate of waiver. This information is not otherwise available to DHS.

5. ***If the collection of information has a significant impact on a substantial number of small businesses or other small entities (Item 5 of the Paperwork Reduction Act submission form), describe the methods used to minimize burden.***

The information collection discussed in this analysis applies to States, State agencies, and certain employees involved in process to apply for a temporary certificate of waiver. Therefore, it is DHS's belief that the information collection does not have a significant impact on a substantial number of small businesses or other small entities.

6. ***Describe the consequence to Federal program or policy activities if the collection is not conducted or is conducted less frequently, as well as any technical or legal obstacles to reducing burden.***

The collection of the information will enable DHS to issue a waiver to States, which would authorize Federal agencies to accept, at their discretion, a State's mDL for official purposes. Without this information collection, under 6 CFR 37.5(b), mDLs issued by States will be not be accepted by Federal agencies for official purposes beginning May 7, 2025. As discussed in response to Question 1 above, mDLs potentially provide significant security benefits to Federal agencies. Without this information collection, Federal agencies would be prohibited from accepting mDLs on May 7, 2025, thereby depriving them of this potential security enhancement.

The proposed rule, and therefore this collection, also supports DHS's commitment to Executive Order 14058 of December 13, 2021 (Transforming Federal Customer Experience and Service Delivery to Rebuild Trust in Government). This EO focused on enhancing the use of technology "to modernize Government and implement services that are simple to use, accessible, equitable, protective, transparent, and responsive for all people of the United States." The Secretary of Homeland Security has specifically committed to testing the use of mDLs to establish identity at airport security checkpoints, which would provide the public with increased convenience from reduced wait times, security, privacy, and health benefits from "contact-free" identity verification.

7. Explain any special circumstances that require the collection to be conducted in a manner inconsistent with the general information collection guidelines in 5 CFR 1320.5(d)(2).

This collection is conducted consistent with the information collection guidelines, except for those in 5 CFR 1320.5(d)(2)(i). This collection requires respondents to report information to the agency more often than quarterly. Quarterly reporting would not meet the security needs that is the basis for this information collection.

8. Describe efforts to consult persons outside the agency to obtain their views on the availability of data, frequency of collection, the clarity of instructions and recordkeeping, disclosure, or reporting format (if any), and on the data elements to be recorded, disclosed, or reported. If applicable, provide a copy and identify the date and page number of publication in the *Federal Register* of the agency's notice, required by 5 CFR 1320.8(d) soliciting comments on the information collection prior to submission to OMB. Summarize public comments received in response to that notice and describe actions taken by the agency in response to these comments. Specifically address comments received on cost and hour burden.

In April 2021, DHS issued a Request for Information⁷ (RFI) announcing DHS's intent to commence future rulemaking to set the minimum technical requirements and security standards for mDLs to enable Federal agencies to accept mDLs for official purposes. The RFI requested comments and information to inform DHS's rulemaking. In June 2021, DHS held a public meeting⁸ to provide an additional forum for comment, and extended the comment period. In response to comments at the public meeting concerning the importance of public access to an industry-developed standard referenced in the RFI, DHS subsequently published a notice⁹ in the *Federal Register* to facilitate access to the standard, and further extended the comment period. The RFI requested comments on 13 specific topics, including: potential security risks arising from mDL usage and mitigating solutions, potential privacy concerns or benefits associated with mDL transactions, the maturity of certain industry standards and the appropriateness of DHS's adoption of them, costs to individuals to obtain mDLs, and various technical topics associated with mDL issuance and communications.

⁷ 86 FR 20320 (April 19, 2021).

⁸ 86 FR 31987 (June 16, 2021).

⁹ 86 FR 51625 (Sept. 16, 2021).

DHS received roughly 60 comments to the RFI from a diverse group of stakeholders, including advocacy groups representing varied interests, individuals, State government agencies, trade associations, and industry. An analysis of comments received showed that topics of interest to stakeholders concerned: the need for standardization and/or Federal guidance, potential benefits to the public from mDLs generally, and the appropriateness of certain industry standards as a starting point for regulatory requirements.

DHS has also conducted extensive outreach and engagement with affected stakeholders, including States, industry, and individuals. In addition, DHS conducted a roundtable discussion on privacy considerations with non-profit organizations representing varied interests.

DHS published an NPRM, seeking comments on 9 specific topics as well as general comments on the NPRM. *See* 88 FR 60056 (August 30, 2023). TSA received 31 comments,¹⁰ including some comments that were submitted shortly after the comment period closed. TSA accepted every comment received as part of the official record, including those that were submitted late. Following careful consideration of all public comments received, TSA made some modifications to the regulatory text proposed in the NPRM, as noted in the final rule.

In addition, TSA published a 30-day notice in the *Federal Register* to solicit public comment on the information collection. *See* 89 FR 77536 (September 23, 2024). TSA received no public comment on the information collection.

9. *Explain any decision to provide any payment or gift to respondents, other than remuneration of contractors or grantees.*

DHS will not provide any payment or gift to respondents.

10. *Describe any assurance of confidentiality provided to respondents and the basis for the assurance in statute, regulation, or agency policy.*

While there is no assurance of confidentiality, information provided will be protected from disclosure to the extent appropriate under applicable provisions of the Freedom of Information Act, the Privacy Act of 1974, the Driver's Privacy Protection Act, as well as DHS's Privacy Impact Assessment for the REAL ID Act.

11. *Provide additional justification for any questions of sensitive nature, such as sexual behavior and attitudes, religious beliefs, and other matters that are commonly considered private.*

DHS will not ask any questions of a sensitive nature.

¹⁰ The 31 total comments include 1 duplicate, 1 correction, and 1 confidential submission.

12. Provide estimates of hour and cost burdens of the collection of information.

The proposed rule would require the following information collections from States:

- (a) Submission of an initial waiver application, including audit report;
- (b) Supplemental submissions for applications deemed insufficient;
- (c) Requests for reconsideration of applications subject to a notice of denial;
- (d) Submission of a new application for: initial applications that have been denied, to renew an expired waiver, or waivers that have been suspended or terminated;
- (e) Reporting requirements for significant modifications that a State makes to its mDL issuance processes that materially differ from information that the State provided in its application that was the basis of an issued waiver;
- (f) Reporting requirements for discovery of a significant cyber incident or breach which may compromise the integrity of State Certificate Systems; and
- (g) Responses to DHS notices of suspension or termination.

All fifty States, the District of Columbia, and five territories (collectively “States”) are eligible to voluntarily apply for a mDL waiver. However, DHS assumes that not all States eligible for the mDL waiver would apply. Some States have not taken action towards mDL implementation, and there may be States whose mDL setup or philosophy would lend them towards waiting until the mDL ecosystem is more fully developed. As a result, DHS believes some, but not all, States will request a mDL waiver. Specifically, DHS assumes 15 States would apply for a mDL waiver in year 1 of the analysis, 10 States in year 2, and 5 States in year 3, a total of 30 responses over a three-year period and an average of 10 annual responses.

After submission of the mDL waiver application and a DHS review, DHS can make one of three determinations on the request for a mDL waiver: approval, insufficient, or denial. States can amend an insufficient waiver application and resubmit for DHS review or submit a new application if the initial application is denied. DHS anticipates all initial mDL waiver applications would receive a determination of insufficient. However, DHS intends to work with States to meet the mDL application criteria and as a result does not anticipate any applications being denied. As a result, States would not submit any new applications as a result of a denial or a request for reconsideration of a denied application. However, DHS assumes only 90 percent of applicants will resubmit their waiver applications initially deemed insufficient with the remaining percentage of applicants not continuing to pursue a mDL waiver and waiting until the mDL environment is more fully developed. Therefore, DHS assumes 13.5 States would resubmit their waiver applications in year 1, 9 States in year 2, and 4.5 States in year 3, a total of 27 responses over a three-year period and an average of 9 annual responses.

A State’s mDL waiver would be valid for three years. Therefore, States granted a mDL waiver in Year 1 would need to submit a mDL waiver reapplication in Year 4 of the analysis.

DHS technology subject matter experts (SMEs) estimate that the initial mDL waiver application would take, on average, 20 hours to complete. DHS also estimates that mDL

waiver resubmissions would take 25 percent of the initial mDL waiver application time, which equates to 5 hours.¹¹

DHS does not possess sufficient information to estimate the frequency of potential or actual suspensions or terminations of a State's mDL waiver or the frequency of reporting related to material changes or threats to security, privacy, or data integrity. DHS assumes there would not be more than 9 collections related to reporting or responses to DHS notices of suspensions or terminations, and as such, these collections would not be subject to the PRA. Events related to reporting or waiver suspensions and terminations likely have a low probability of occurrence. In addition, DHS estimates only 30 States would submit a mDL waiver application over the three-year period. DHS will provide more data on the frequency and burden of suspensions, terminations, and reporting upon the renewal of this information collection.

DHS estimates the total three-year burden for mDL waiver applications and mDL waiver resubmissions is 57 responses and 735 hours. DHS estimates an average yearly burden of 19 responses and 245 hours.

DHS assumes a weighted average hourly compensation rate of \$76.90¹² for the State employees that would submit the information collections. DHS estimates States would incur a total cost of \$56,518 to submit the information collections in the first three years of the analysis. This equates to an annual average cost of \$18,839. Details of the calculations can be found in the following table.

Table 1: Information Collection Responses, Burden Hours, and Burden Costs

Year	Collection Activity ¹³			Total Burden Hours	Wage Rate	Time Burden Cost
	Waiver Applications	Waiver Resubmissions	Total Responses			
	a	b	c = a + b			
Year 1	15	13.5	28.5	d = (a×20) + (b×5)	e = \$76.90	f = d × e
Year 2	10	9	19			
Year 3	5	4.5	9.5			
Total	30	27	57	735.0		\$56,518

¹¹ mDL waiver resubmission burden = 20 hours [initial mDL waiver application burden] x 0.25 = 5 hours.

¹² DHS uses the following fully-loaded, average hourly compensation rates for the labor categories within State government that would complete a mDL waiver application: \$64.62 for a solutions architect, \$86.82 for an IT manager, \$100.63 for the administrator of the Department of Motor Vehicles, and \$74.34 for a lawyer. DHS estimates for a mDL waiver application, a solutions architect and IT manager would each comprise 45 percent of the total time burden, while the administrator and lawyer would each account for 5 percent. DHS multiplies the average hourly compensation rates by the proportion of each labor category's burden to complete a mDL waiver application to calculate the weighted average hourly compensation per mDL waiver application. \$76.90 weighted average hourly compensation = (\$64.62 per hour for solutions architect x 45 percent) + (\$86.82 per hour for IT manager x 45 percent) + (\$100.63 per hour for administrator x 5 percent) + (\$74.34 per hour for lawyer x 5 percent).

¹³ The table excludes all other information collections. DHS assumes 9 or fewer collections over the three-year period for reconsideration, mDL waiver reapplications, reporting of modifications, reporting of cyber incidents, and responses to DHS notices of suspension or termination.

Average	10	9	19	245.0		\$18,839
---------	----	---	----	-------	--	----------

13. Provide an estimate of the total annual cost burden to respondents or record-keepers resulting from the collection of information.

States would also incur costs associated with independent entity audits of their mDL infrastructure. States would incur this cost for each initial mDL waiver application. DHS estimates this independent entity audit cost at \$32,500 per waiver application. DHS estimates States would submit 30 waiver applications in the first three years of the rule, resulting in a total three-year cost of \$0.98 million and an annual average cost of \$0.33 million.¹⁴

14. Provide estimates of annualized cost to the Federal Government. Also, provide a description of the method used to estimate cost, and other expenses that would not have been incurred without this collection of information.

DHS technology SMEs estimate it would take a DHS reviewer, on average, about 40 hours to complete an initial mDL waiver application review and 10 hours to review a resubmitted mDL waiver application that was initially insufficient. DHS also assumes a reviewer compensation rate of \$71.10¹⁵ per hour. DHS estimates DHS would incur a total cost of \$104,511¹⁶ in the first three years of the analysis and an average annual cost of \$34,837.

15. Explain the reasons for any program changes or adjustments reported in Items 13 or 14 of the OMB Form 83-I.

There has been no program changes or new requirements established as a result of this collection request.

16. For collections of information whose results will be published, outline plans for tabulation and publication. Address any complex analytical techniques that will be used. Provide the time schedule for the entire project, including beginning and ending dates of the collection of information, completion of report, publication dates, and other actions.

DHS will not publish the results of this collection. DHS will only publish the names of States that have been issued a certificate of waiver.

¹⁴ Total three-year audit cost of \$0.98 million would equal the 30 waiver applications multiplied by the \$32,500 audit cost per waiver application. The average annual audit cost of \$0.33 million would equal the total three-year audit cost of \$0.98 million divided by three.

¹⁵ DHS assumes that the equivalent of a GS-13 employee would review mDL waiver applications. DHS estimates an annual fully-loaded compensation of \$148,377, based on the sum of all Personnel Compensation and Benefits for GS-13 Employees (\$109,508 in wages and \$38,869 in benefit compensation). DHS divides the annual fully-loaded compensation of \$148,377 by 2,087 annual work hours to calculate an hourly compensation rate of \$71.10.

¹⁶ Total DHS cost of \$104,511 = ((30 total waiver applications x 40 hours) + (27 total waiver resubmissions x 10 hours)) x \$71.10 per hour.

17. If seeking approval to not display the expiration date for OMB approval of the information collection, explain the reasons why display would be inappropriate.

All information gathered under this collection will be in formats governed by individual State requirements and formats, thus display of the OMB number would be inappropriate.

18. Explain each exception to the certification statement identified in Item 19, "Certification for Paperwork Reduction Act Submissions," of OMB Form 83-I.

DHS is not seeking any exceptions.